UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA

JEFF BUONGIORNO, **CASE NO.: 9:24-cv-80920-AMC**

Plaintiff,

v.

ALEJANDRO MAYORKAS, et al,

Defendants.

EMERGENCY SUBPOENA

TO PRODUCE DOCUMENTS OR ELECTRONICALLY STORED INFORMATION

TO:

WENDY SARTORY LINK
PALM BEACH COUNTY SUPERVISOR OF ELECTIONS
4301 CHERRY ROAD
WEST PALM BEACH, FL 33416

YOU ARE HEREBY COMMANDED, pursuant to Rule 45 of the Federal Rules of Civil Procedure, to produce the following documents or electronically stored information in your possession, custody, or control **on an expedited and emergency basis**:

Documents and Information Requested:

1. **All records of originating IP addresses** associated with **Vote-by-Mail (VBM) ballot requests** in **PALM BEACH COUNTY** for the **2024 Primary Election** and **2024 General Election**.

Expedited Date and Location for Production:

The requested documents and electronically stored information must be produced **no later than November 1st, 2024**, and delivered to:

Jeff Buongiorno
1901 South Congress Ave

Boynton Beach, Fl 33426
561-690-0430
jeff@etektraining.com

Failure to comply with this subpoena may result in legal penalties under Rule 45(g) of the Federal Rules of Civil Procedure.

CERTIFICATION

I, **Jeffrey Buongiorno**, certify that this request is being made in good faith and is reasonably necessary for the purpose of investigating the election processes for the **2024 Primary and General Elections** in the state of Florida, particularly in **Palm Beach**. Given the time-sensitive nature of this investigation, expedited production of the requested documents is essential.

Dated this Third Day of October

Respectfully submitted,

Signed____________________________
Jeff Buongiorno
Jeff@etektraining.com

This request includes, but is not limited to:

1. The originating IP addresses associated with each vote-by-mail ballot request in the specified counties.
2. The date and time of the requests.
3. Any metadata related to the requests that may identify the method by which the request was made (e.g., online submission).

2. **Any and all records or documentation reflecting the digital origin or source** of the requests for vote-by-mail ballots submitted electronically from **PALM BEACH COUNTY** including logs of submission dates and associated IP addresses for the **2024 Primary Election** and **2024 General Election.**

Facts supporting the Motion:

3. **Plaintiff asserts that Defendant Link, through her own admission does not verify UNITED STATES citizenship of newly registered voters in violation of Florida Statutes.** [1]

4. **WHEREAS, VR SYSTEMS has known vulnerabilities, including to the well-known breach of their systems in 2016 by Russian Hackers (Exhibit A, Video Footage).**

[1] FS 97.041 & Sunshine law 1S 2.039 (5) Verification of personal identifying number. Any valid application for new registration that is complete and submitted other than electronically through DHSMV shall be routed to DHSMV or SSA, whichever is applicable, for verification of the authenticity or nonexistence of the PIN provided on the application. However, no application shall be routed to DHSMV for verification unless the Supervisor first determines that the applicant is otherwise eligible in accordance with Section 97.041, F.S.

5. **WHEREAS, VR Systems experienced yet another outage on the first day of early voting in Florida. The outage came only 4 days after Plaintiff notified Defendants BYRD and LINK of newly detected Ransomware related to the VR Systems infrastructure, [2] via electronic mail (Exhibit B)**

[2] https://www.tampabay.com/news/florida-politics/elections/2024/10/21/many-florida-election-office-websites-crashed-first-day-early-voting/

Exhibit A: Video created by Plaintiff posted on Plaintiff's Rumble Channel. Includes Leon County Former Supervisor of Elections statement confirming VR Systems was penetrated by foreign actors during the 2016 Election. The video also includes screenshots of email sent on October 17th, 2024 informing Defendants BYRD and LINK of newly found malicious threat vector. Approximately 5 minutes.

https://rumble.com/v5jiffd-leon-county-supervisor-of-elections-exposes-floridas-election-issues.html

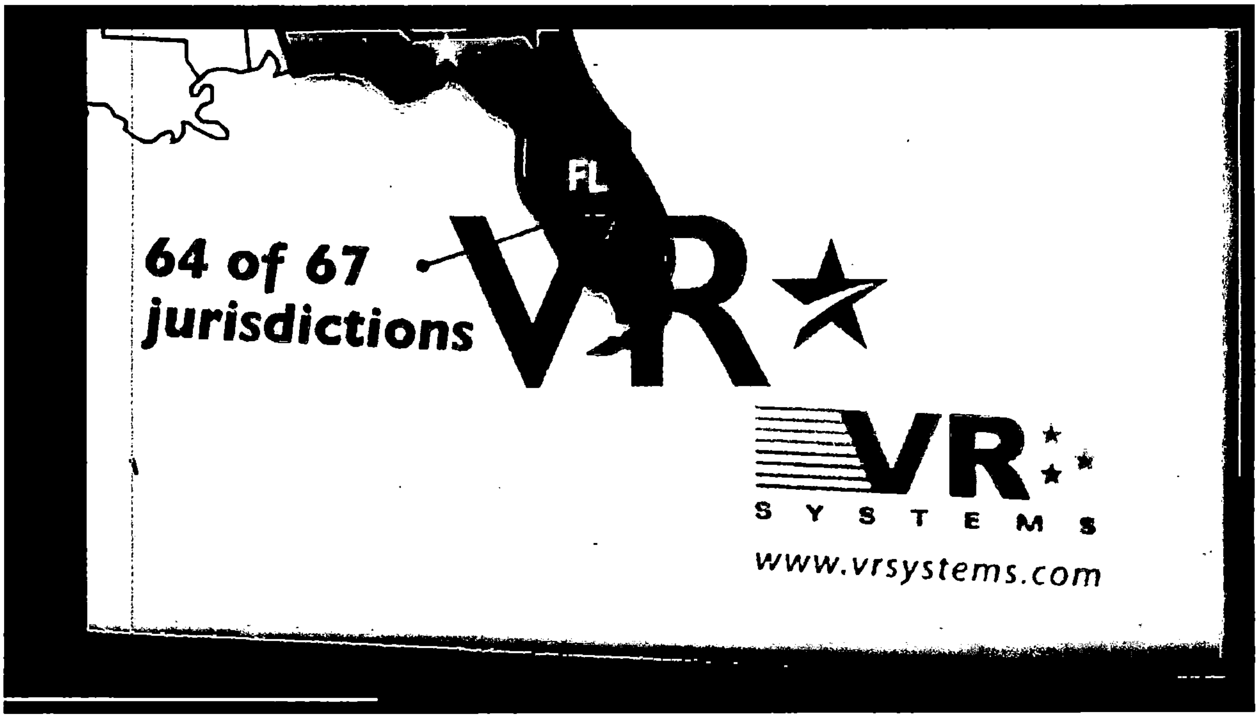
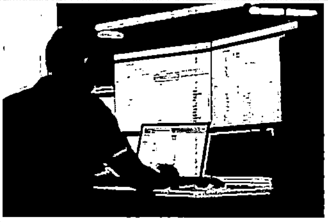


Exhibit B: Email to Link and Byrd. 4 pages

Exhibit B Page 3

MiniDumpWriteDump via COM+ Services DLL | modexp (wordpress.com)

This type of attack has the footprint and markings of Iranian APT Teams AKA REALLY BAD GUYS.
Profiling DEV-0270: PHOSPHORUS' ransomware operations | Microsoft Security Blog



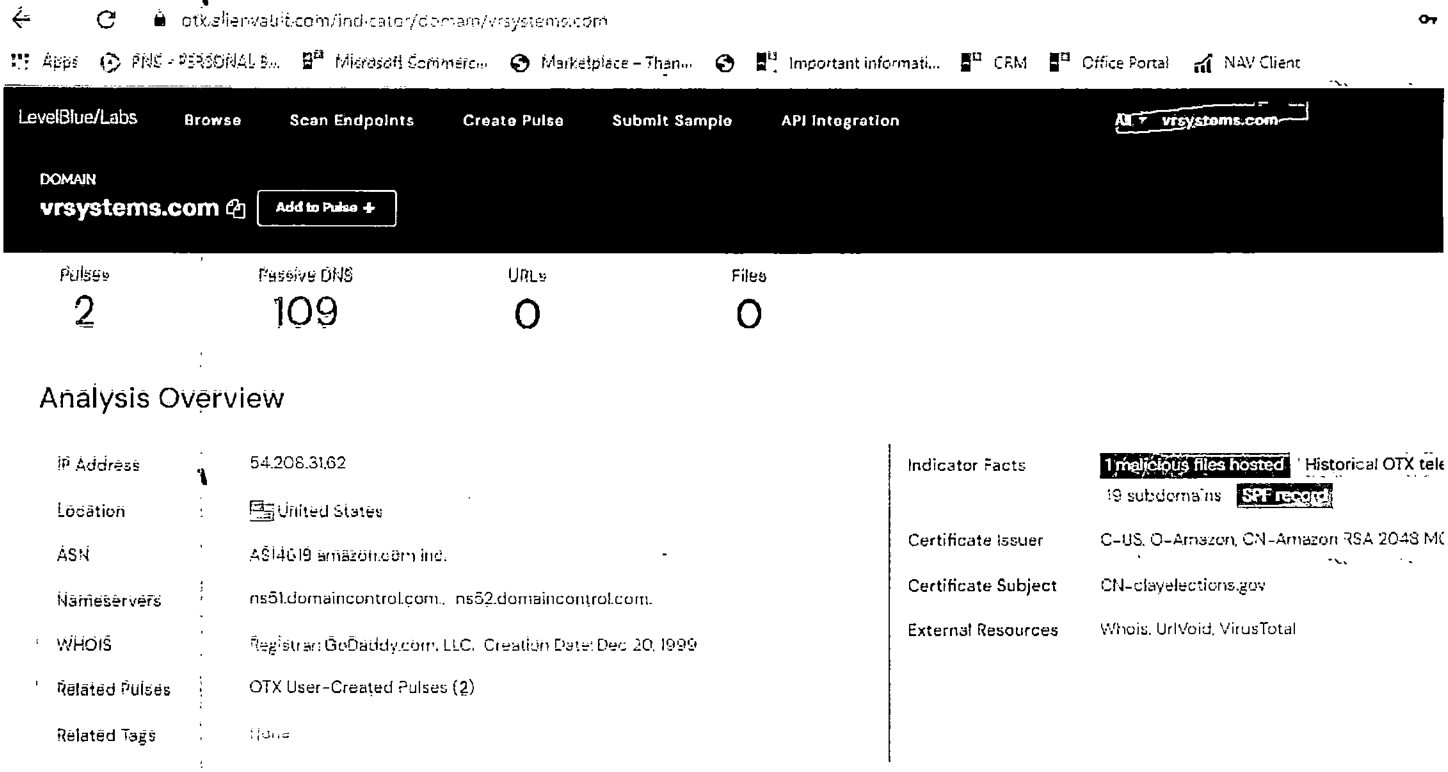
Profiling DEV-0270: PHOSPHORUS' ransomware operations | Microsoft Security Blog

Microsoft threat intelligence teams have been tracking multiple ransomware campaigns tied to DEV-0270, also known as Nemesis Kitten, a sub-group of Iranian actor PHOSPHORUS.

www.microsoft.com

Additionally, virus protection software often will not detect these types as attacks as they are embedded in DLL files that are signed off as safe by the Microsoft Corporation. I know this as I spent four years on the Microsoft Partner Research Panel and through cyber-security and forensics experience.

As an additional point of reference, please see the scan and results found on the Open Threat Exchange (OTX). Our friends at CISA are familiar with this tool.



DOMAIN
vrsystems.com

Pulses	Passive DNS	URLs	Files
2	109	0	0

Analysis Overview

IP Address	54.208.31.62
Location	United States
ASN	AS14619 amazon.com inc.
Nameservers	ns51.domaincontrol.com., ns52.domaincontrol.com.
WHOIS	Registrar: GoDaddy.com, LLC, Creation Date: Dec 20, 1999
Related Pulses	OTX User-Created Pulses (2)
Related Tags	None

Indicator Facts	1 malicious files hosted Historical OTX tele 19 subdomains SPF record
Certificate Issuer	C=US, O=Amazon, CN=Amazon RSA 2048 M(
Certificate Subject	CN=clayelections.gov
External Resources	Whois, UrlVoid, VirusTotal

I will not offer any guidance on the subject, although we all what the prudent course of action is. We can let the folks at CISA tell you that there is nothing to see here at the bequest of their impeached leader, Alejandro Mayorkas, who is also a defendant in complaint filed by the State of Florida just one day ago.
https://www.msn.com/en-us/news/us/biden-admin-slapped-with-major-lawsuit-over-alleged-refusal-to-help-state-purge-noncitizens-from-voter-rolls/ar-AA1srsfl

Biden admin slapped with major lawsuit over alleged refusal to help state purge noncitizens from voter rolls

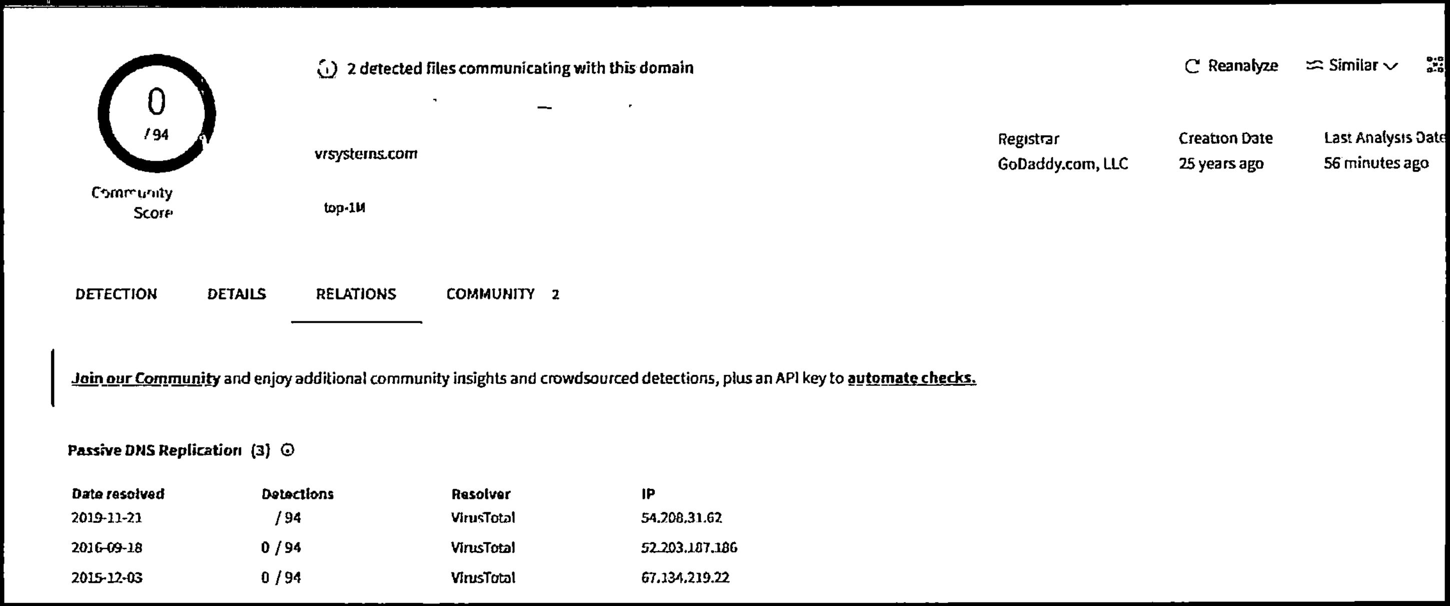
Florida is suing the Biden administration over what it alleges is a refusal by the Department of Homeland Security to aid in its efforts to remove noncitizens from the voter rolls.

www.msn.com

Important to note: Ransomware is not always intended to collect a Ransom. Ransom can go undetected for long durations and are used to compromise a system for purposes such as escalating user privileges, as an example.

Finally, a relevant article regarding ransomware:
https://www.wxyz.com/news/wayne-county-services-in-disarray-as-officials-continue-to-work-through-cyberattack\

Exhibit B PAGE 2



2 detected files communicating with this domain

vrsystems.com

top-1M

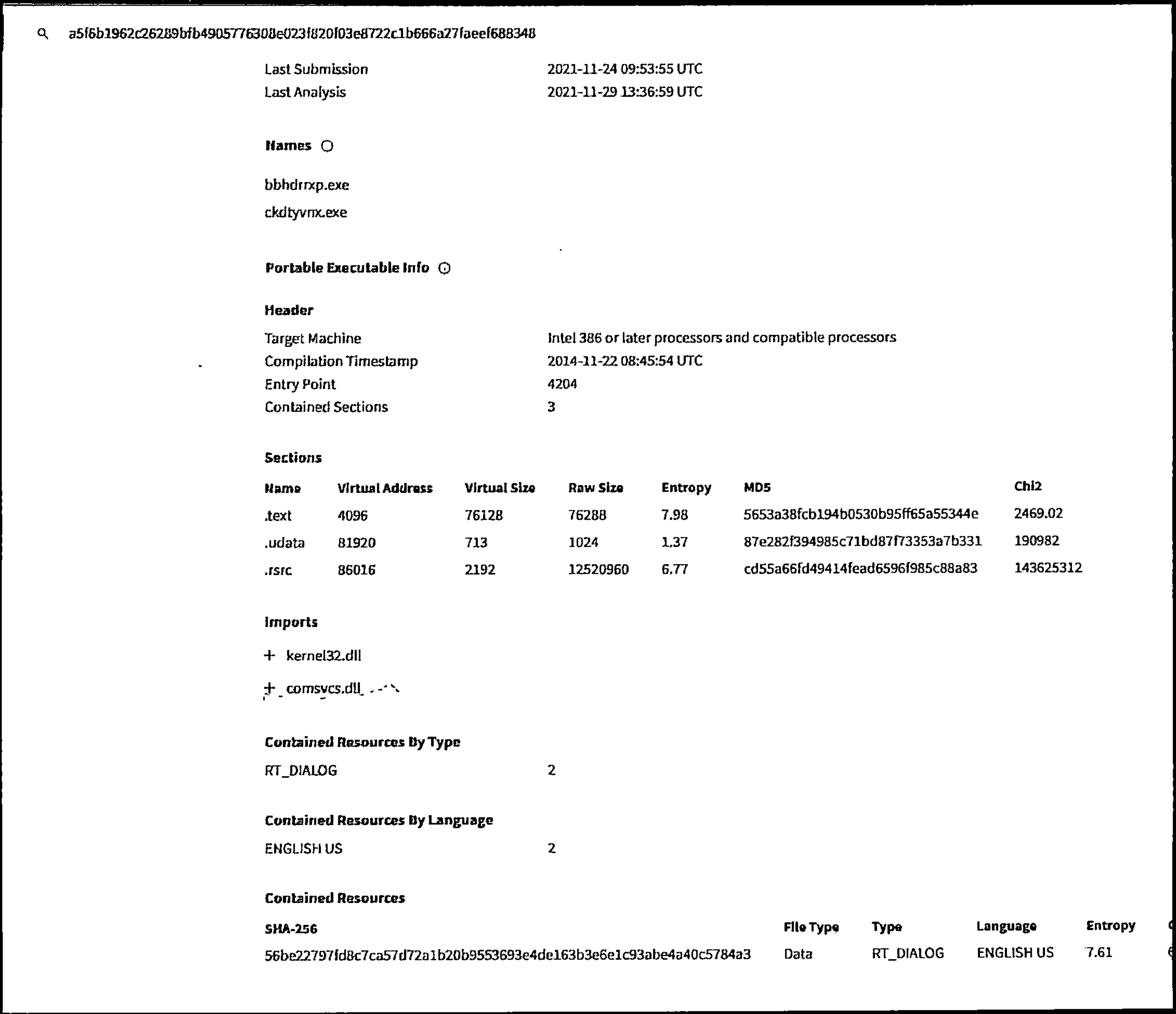
Registrar	Creation Date	Last Analysis Date
GoDaddy.com, LLC	25 years ago	56 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (3)

Date resolved	Detections	Resolver	IP
2019-11-21	/ 94	VirusTotal	54.208.31.62
2016-09-18	0 / 94	VirusTotal	52.203.187.186
2015-12-03	0 / 94	VirusTotal	67.134.219.22

The DLL (Dynamic Link Library) impacted by the .EXE shown here: We will focus on comsvcs.dll only.



a5f6b1962c26289bfb4905776308e023f820f03e8722c1b666a27faeef688348

Last Submission	2021-11-24 09:53:55 UTC
Last Analysis	2021-11-29 13:36:59 UTC

Names

bbhdrrxp.exe

ckdtyvnx.exe

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2014-11-22 08:45:54 UTC
Entry Point	4204
Contained Sections	3

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	76128	76288	7.98	5653a38fcb194b0530b95ff65a55344e	2469.02
.udata	81920	713	1024	1.37	87e282f394985c71bd87f73353a7b331	190982
.rsrc	86016	2192	12520960	6.77	cd55a66fd49414fead6596f985c88a83	143625312

Imports

+ kernel32.dll

+ comsvcs.dll

Contained Resources By Type

RT_DIALOG	2

Contained Resources By Language

ENGLISH US	2

Contained Resources

SHA-256	File Type	Type	Language	Entropy
56be22797fd8c7ca57d72a1b20b9553693e4de163b3e6e1c93abe4a40c5784a3	Data	RT_DIALOG	ENGLISH US	7.61

Below is a link showing how comsvc.exe can be manipulated to Elevate User privileges or access level in the system by impacting LSASS.EXE (local security authority subsystem services).

Exhibit B PAGE 1

Outlook

VRSYSTSTEMS seemingly infected Iranian APT TEAM DEV-0270

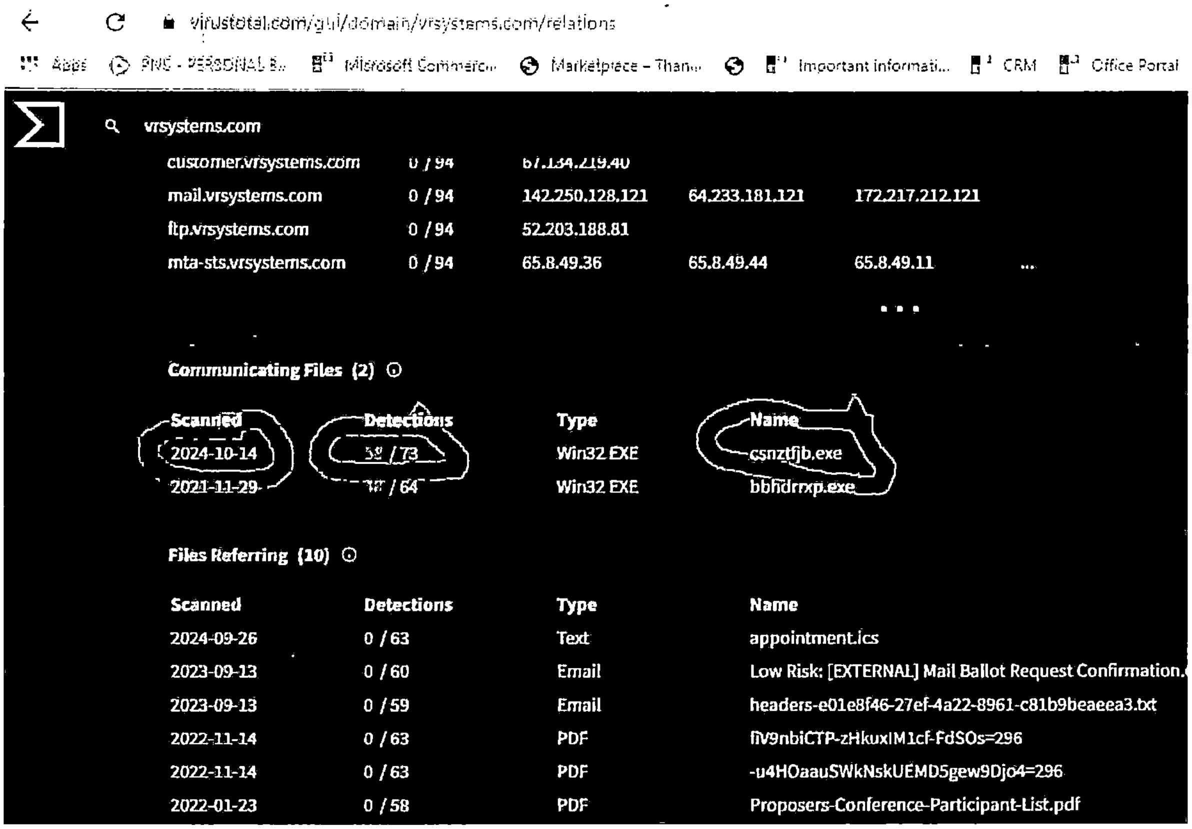
From Jeff Buongiorno <Jeff@etektraining.com>
Date Thu 10/17/2024 10:29 PM
To wendy@votepalmbeach.gov <wendy@votepalmbeach.gov>; Cord Byrd <cord.byrd@dos.myflorida.com>
Cc tbuffington1 <tbuffington1@protonmail.com>; kjmeckert@protonmail.com <kjmeckert@protonmail.com>; Kevin Neal <neal.kj@gmail.com>; Carl Cascio <casciolaw@comcast.net>; jenine@jeninemilum.com <jenine@jeninemilum.com>; Kelly Collins <kelly@kellyecollins.com>; Raj Doraisamy <raj@defendourunion.org>; Christopher Gleason <cpgleason72@gmail.com>; Bob Guzzardi <bob.guzzardi@gmail.com>; Joseph Korff <josephkorff@icloud.com>; Erin Aktas <erinrdhsmile@gmail.com>; Bernie Jessen <hsryard@aol.com>; 'Ralph98' <gibbstown98@yahoo.com>; Jeff Crouere <jcrouere@gmail.com>; 'Ann Vandersteel' <ann@annvandersteel.com>; contact@Donna4Mi.com <contact@donna4mi.com>; Anthony Man <aman@sunsentinel.com>; dclyons@gannett.com <dclyons@gannett.com>; Steve Bousquet <sbousquet@sunsentinel.com>; adam.shaw2@fox.com <adam.shaw2@fox.com>
Bcc [redacted]

Dear Ms. Link & Secretary Byrd,

In your last email, you offered confirmation that VirusTotal.com is a trusted tool used for rooting out cyber threats. You went as far as introducing their Knowledge Base Articles as a trusted source. Finally, something we can both agree on!

Virustotal.com is trusted by CISA as per your last email.

A virustotal.com scan of the domain "VRSYSTEMS.COM" suggests that the domain contains Ransomware. An executable was found on October 14th, 2024 as you can see in the first image below, csnztfjb.exe. There are two, I will only focus the one highlighted below. Perhaps our "friends" CISA can expand on the second threat.



customer.vrsystems.com	0 / 94	67.134.219.40			
mail.vrsystems.com	0 / 94	142.250.128.121	64.233.181.121	172.217.212.121	
ftp.vrsystems.com	0 / 94	52.203.188.81			
mta-sts.vrsystems.com	0 / 94	65.8.49.36	65.8.49.44	65.8.49.11	...

Communicating Files (2)

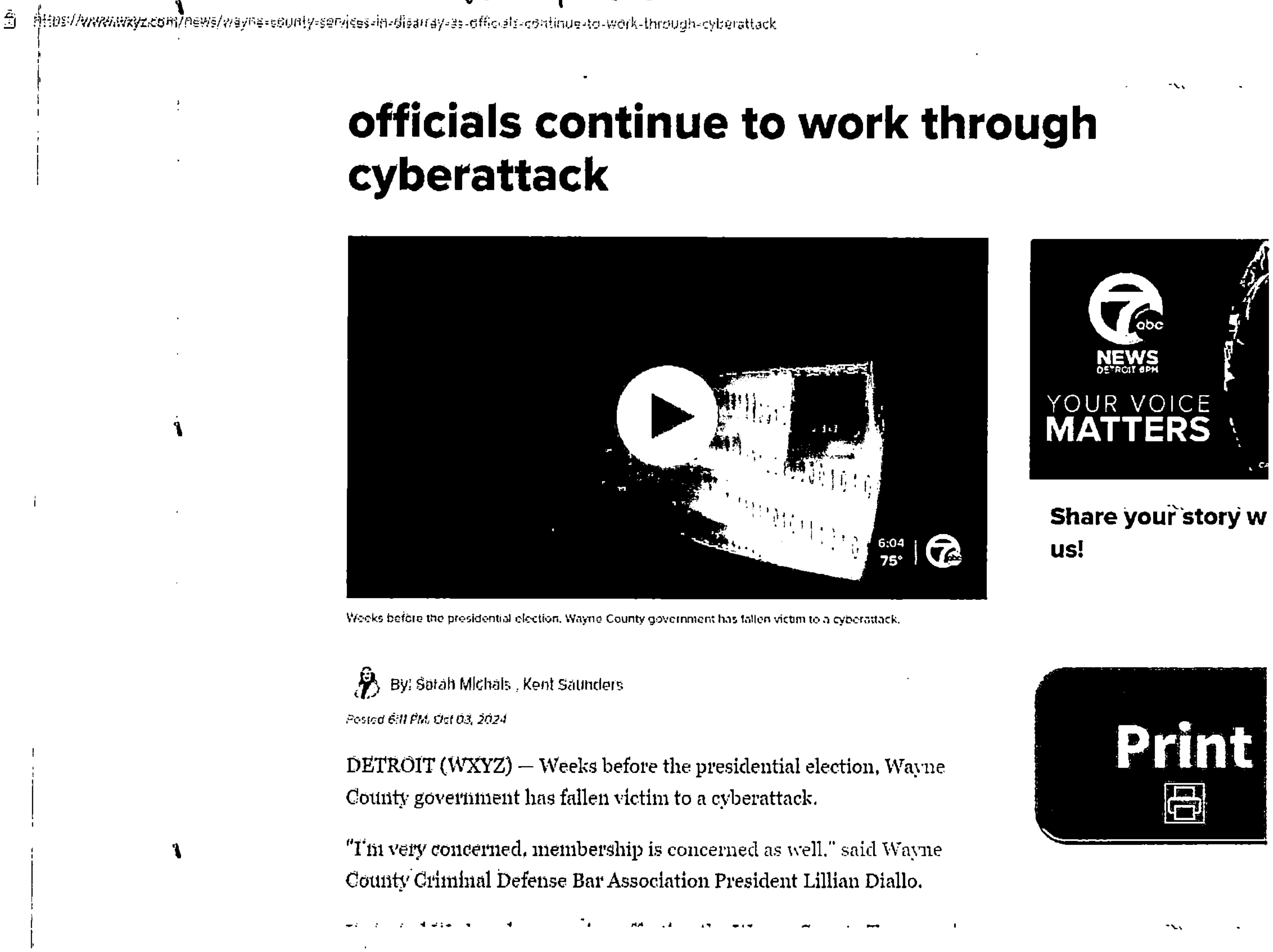
Scanned	Detections	Type	Name
2024-10-14	59 / 73	Win32 EXE	csnztfjb.exe
2021-11-29	[illegible] / 64	Win32 EXE	bbhdrrxp.exe

Files Referring (10)

Scanned	Detections	Type	Name
2024-09-26	0 / 63	Text	appointment.ics
2023-09-13	0 / 60	Email	Low Risk: [EXTERNAL] Mail Ballot Request Confirmation.
2023-09-13	0 / 59	Email	headers-e01e8f46-27ef-4a22-8961-c81b9beaeea3.txt
2022-11-14	0 / 63	PDF	fiV9nbiCTP-zHkuxIM1cf-FdSOs=296
2022-11-14	0 / 63	PDF	-u4HOaauSWkNskUEMD5gew9Djo4=296
2022-01-23	0 / 58	PDF	Proposers-Conference-Participant-List.pdf

IMAGE 2- Confirmation that there are two files communicating with this domain.

Exhibit B Page 4



https://www.wxyz.com/news/wayne-county-services-in-disarray-as-officials-continue-to-work-through-cyberattack

officials continue to work through cyberattack

Weeks before the presidential election, Wayne County government has fallen victim to a cyberattack.

By: Sarah Michals , Kent Saunders

Posted 6:11 PM, Oct 03, 2024

DETROIT (WXYZ) — Weeks before the presidential election, Wayne County government has fallen victim to a cyberattack.

"I'm very concerned, membership is concerned as well," said Wayne County Criminal Defense Bar Association President Lillian Diallo.

Jeff Buongiorno
E-Tek Software & Services
E-Tek Software & Services
Publisher of ConfigureNow! CPQ as seen on Microsoft App Source
Jeff@etektraining.com